

Практическое пособие для тех, кто хочет превратить DLP-систему в эффективный инструмент, получить повышение и укрепить статус службы ИБ в компании

Хотите превратить проект по DLP из головной боли в достижение, достойное резюме? Упрочить свое положение в компании и помочь самой компании улучшить бизнес-показатели? Тогда это руководство – для вас!

DLP-системы – один из самых сложных классов корпоративных решений по информационной безопасности. Внедрение и эксплуатация DLP требует не только знаний и умений, но и опыта, который нельзя получить, не поработав с аналогичными системами. Специфичность DLP-систем обусловлена их тесной интеграцией с другими корпоративными системами и отлаженными бизнес-процессами. При этом сложности могут возникнуть на любом этапе. Руководство аккуратно проведет по всем этапам проекта по DLP, от получения бюджета до настройки конкретного решения и запуска его в промышленную эксплуатацию.

Данное пособие предназначено для специалистов по защите информации, руководителей подразделений по информационной безопасности, топ-менеджмента компаний, озадаченных вопросами предотвращения утечек информации (DLP) по электронным каналам. Пособие дает исчерпывающие ответы на вопросы, как выбрать DLP-систему и как ее настроить, чтобы быстро окупить потраченные средства, как правильно внедрить и как юридически грамотно обосновать использование в своей организации, как вычислить потенциального инсайдера и предотвратить утечку важной информации задолго до того, как она произойдет.

Особую ценность представляют практические рекомендации на основе многолетнего опыта авторов и сотен реализованных проектов в сфере защиты информации от утечек. А приведенные в приложениях типовые формы и шаблоны документов окажут помощь в работе над вашим собственным проектом по DLP.

Краткое изложение

Глава 1. Готовы ли мы к импортозамещению в области DLP

- 1.1. Развитие технологий предотвращения утечек
- 1.2. Архитектура и состав DLP-систем
- 1.3. Современная ситуация на российском рынке DLP

Глава 2. Используем DLP легально и открыто

- 2.1. Несколько слов о европейской практике
- 2.2. Российские особенности
- 2.3. Как подготовить почву для внедрения DLP
- 2.4. Заключительные рекомендации

Глава 3. Как выбрать наиболее подходящую DLP-систему

- 3.1. Трудности выбора
- 3.2. Критерии оценки DLP-систем
 - Каналы передачи данных
 - Технологии распознавания
 - Режимы работы
 - Архив и инструменты для его анализа
 - Управление и отчетность

Глава 4. Секреты эффективности DLP-систем

- 4.1. Типичные ошибки при внедрении DLP
- 4.2. Типичные ошибки при обслуживании DLP
- 4.3. Как не попасть в ловушку низкой цены
- 4.4. Сферы использования DLP
- 4.5. О сертифицированных DLP-системах

Глава 5. Внедрение DLP своими силами

5.1. Объективные сложности

5.2. Борьба с техническими и организационными проблемами

5.3. Избегаем типичных ошибок

Глава 6. Поиск инсайдеров и сбор цифровых улик

6.1. Что хранить в архиве

6.2. Как DLP облегчает расследование

6.3. Расследовать, чтобы предотвращать

Глава 7. Как получить финансирование проекта по ИБ

7.1. Пять принципов, которые помогут добиться результата

7.2. Не усложнять проект

7.3. Решение проблем, а не функционал

7.4. Нефинансовая мотивация

7.5. Финансовая выгода в цифрах

7.6. Просить больше

Приложение 1. Техническое сравнение DLP-систем

Общая информация

- *Режимы работы*
- *Режимы перехвата информации*
- *Возможности интеграции*
- *Производительность и отказоустойчивость*

Контролируемые каналы

- *Электронная почта*
- *Контролируемые каналы. Системы мгновенного обмена сообщениями*
- *Контролируемые каналы. Протокол HTTP и его модификации*
- *Контролируемые каналы. FTP, P2P*
- *Контролируемые каналы. Туннелирующие протоколы*
- *Контролируемые каналы. Внешние устройства*
- *Контролируемые каналы. Мобильные устройства*
- *Контролируемые каналы. Прочие протоколы*

Мониторинг и защита агентов

Контроль пользователей

Поиск конфиденциальной информации в сети предприятия

Реакция на инциденты

Аналитические возможности

Хранение, ретроспективный анализ и отчетность

Итоги технического сравнения

Выводы

Приложение 2. Типовой порядок ввода DLP-системы в эксплуатацию

Приложение 3. Типовые цели внедрения DLP-системы

Назначение DLP-систем

Цели внедрения DLP-систем

Задачи, решаемые при внедрении DLP-систем

Приложение 4. Типовой шаблон программы и методики испытаний

Объект испытаний

Цели испытаний

Объем испытаний

Требования к системе
Требования к программной документации
Состав и порядок испытаний
Методы испытаний

Приложение 5. Типовые требования, предъявляемые к DLP-системам

Основные требования к структуре и функционированию DLP-систем
Требования к контролю доступа
Требования к задачам, решаемым DLP-системой

Приложение 6. Типовой порядок испытаний и приемки DLP-системы

Общие требования к испытаниям
Условия опытной эксплуатации DLP-системы
Передача DLP-системы заказчику
Общие требования к приемке работ

Приложение 7. Типовой план-график работ по внедрению DLP-системы

Приложение 8. Шаблон положения о коммерческой тайне (КТ)

Общие положения
Перечень сокращений
Термины и определения
Организация защиты коммерческой тайны лиц, допущенных к коммерческой тайне
Организация конфиденциального делопроизводства
Обязанности лиц, допущенных к коммерческой тайне
Ответственность за разглашение коммерческой тайны

Приложение 9. Шаблон перечня сведений, составляющих КТ

Приложение 10. Шаблон списка лиц, имеющих доступ к КТ

Приложение 11. Шаблон соглашения о неразглашении КТ с сотрудником

Приложение 12. Памятка по работе с DLP-системой

Как легализовать внедрение DLP-системы
Базовые критерии выбора DLP-системы
Алгоритм действий офицера безопасности при фиксировании инцидента ИБ
Союзники по эксплуатации DLP-системы
Как успешно внедрить DLP-систему
Проверить себя перед внедрением DLP-системы

Дополнения к диску



1. Построение комплексной системы защиты от утечек конфиденциальной информации BEST PRACTICE DLP



2. Дополнительный цикл публикаций по средствам защиты от утечки конфиденциальной информации (DLP)